Reactie column "Wilt u af van de authenticatiepooier?", FD 06-02-2016

Eric Verheul

Naast mijn deeltijd betrekking als hoogleraar binnen de Digital Security groep ben ik ook onafhankelijk adviseur/auditor rond informatiebeveiliging. In die hoedanigheid ben ik ook betrokken als (cryptografisch) adviseur bij het Idensys programma dat als doel heeft een hoogwaardige elektronische identiteit voorziening binnen Nederland te bereiken. Mijn taak is te adviseren rond een optimale balans tussen drie fundamentele aspecten: betrouwbaarheid (fraudebestendigheid), gebruikersvriendelijkheid en privacy vriendelijkheid. Met name vanuit gebruikersvriendelijkheid is binnen Idensys gekozen voor een zogenaamde federatieve identiteit voorziening. In onderstaande tekst zal ik nader uitleggen wat deze opzet behelst.

De federatieve keuze van de overheid lijkt haaks te staan op een technologie die is ontwikkeld op mijn eigen universiteit namelijk de IRMA kaart. Deze technologie is juist niet-federatief van opzet. Binnen Nederland lijkt een stammenstrijd te zijn ontstaan tussen de federatieve en niet-federatieve opzet. De laatste manifestatie van deze strijd is de column [1.] van mijn Radboud collega Jaap-Henk Hoepman in het Financieel Dagblad met als titel: 'Wilt u af van de authenticatiepooier?' De titel geeft daarbij aan dat de strijd aan het verharden is.

In dit schrijven probeer ik, als "bewoner" van beide kampen, de verschillen en overeenkomsten tussen beide te verduidelijken. Waarbij ik tot de conclusie kom dat het verschil tussen beide kampen eigenlijk helemaal niet zo groot is als men wel denkt.

Zaterdag 6 februari jl. verscheen een column [1.] van mijn Radboud collega Jaap-Henk Hoepman in het Financieel Dagblad met als titel: 'Wilt u af van de authenticatiepooier?' Deze column gaat in op de nationale elektronische identiteit voorziening Idensys (eID Stelsel) en spreekt daar zorgen over uit. Hoewel een aantal van deze zorgen terecht is, berust de belangrijkste zorg mijn inziens op een denkfout van Jaap-Henk.

Wat namelijk lijkt te worden gesuggereerd is dat "federatieve" authenticatie zoals de overheid die met Idensys tijdens de pilots voorstaat, in beginsel minder betrouwbaar zou zijn dan de niet-federatieve opzet die Jaap-Henk voorstelt. In zijn opzet authentiseert een burger zich rechtstreeks bij een dienstverlener met

een authenticatiemiddel zoals een smart card, secure USB-token of smartphone, dus zonder gebruik van een derde partij.

Allereerst is de tegenstelling tussen beide vormen van authenticatie minder groot dan wat Jaap-Henk lijkt aan te geven. Beide vormen zijn namelijk gebaseerd op een 'vertrouwde derde partij' die na zorgvuldige controle van de identiteit van de aanvrager deze het middel overhandigt. Een middel dat gebaseerd is op een *userid/wachtwoord* levert daarbij een laag veiligheidsniveau onder meer omdat het kan worden gekopieerd zonder dat de eigenaar zich daar bewust van is. Daarom focust Idensys ook op de hoge kwaliteit middelen zoals Jaap-Henk die voorstelt en die ook worden vereist vanuit Europa. Zie [2.] en [3.].

Het verschil tussen beide vormen van authenticatie zit niet in het bestaan van een authenticatiedienst of in de kwaliteit van de middelen. Het verschil zit in het *gebruik* van de middelen verstrekt door de authenticatiedienst. In het voorstel van Jaap-Henk maakt de gebruiker rechtstreeks contact met de dienstverlener waar hij wil aanloggen en gebruikt hij het verstrekte middel daarbij. Dat wil zeggen, de authenticatiedienst heeft wel een rol in de verstrekking van het middel maar niet in het gebruik ervan. Overigens speelt in een niet-federatieve opzet de authenticatiedienst wel degelijk een subtiele een rol in de vaststelling of het middel ingetrokken is. Hier zal ik, evenals Jaap-Henk, gemakshalve aan voorbij gaan.

Bij federatieve authenticatie heeft de authenticatiedienst niet alleen een rol in de verstrekking van het middel maar ook in het gebruik ervan richting de dienstverlener. In deze opzet stuurt de dienstverlener de gebruiker namelijk naar de authenticatiedienst en de gebruiker authentiseert zich met het middel bij de authenticatiedienst. Hierna stuurt de authenticatiedienst de gebruiker weer naar de vragende dienstverlener samen met het resultaat van de authenticatie. Dit neemt de vorm aan van een gestandaardiseerd (identiteit) bericht. Deze opzet is vrij gebruikelijk en wordt ook gebruikt bij iDEAL webshop betalingen: in plaats van dat een webshop rechtstreeks contact maakt met het middel (betaalpas) van de klant wordt de klant doorgestuurd naar zijn bank die het contact met het middel maakt.

Terecht stelt Jaap-Henk nu dat men in de federatieve opzet een groot vertrouwen moet hebben in de authenticatiedienst. Immers als een onbetrouwbare partij deze rol zou kunnen vervullen dan zou dat het gevolg kunnen hebben dat een fraudeur namens een burger kan aanloggen. De denkfout die Jaap-Henk mijn inziens evenwel maakt, is dat dit in zijn eigen voorstel anders zou zijn. Die opzet maakt immers ook gebruik van een authenticatiedienst en ook die zou "zomaar" een middel kunnen uitgeven aan een fraudeur dat op andermans naam staat. Met andere woorden, bij zowel de federatieve als de niet-federatieve opzet speelt de authenticatiedienst een fundamentele betrouwbaarheidsrol. Het is precies deze reden dat in 2014 en 2015 Europese verordeningen [3.], [4.] van kracht geworden zijn die zware

eisen stellen aan authenticatiediensten, eisen die ook geadopteerd zijn door Idensys.

Het zorgpunt van Jaap-Henk dat een middel toch zou kunnen worden verstrekt aan een onjuist persoon is ook onderkend in de Idensys risico analyse [5.]. Het lastige van deze situatie is dat de persoon die het betreft veelal niet op de hoogte zal zijn van deze verstrekking. Pas het misbruik van het middel zal hem daarop kunnen wijzen. Dit is vergelijkbaar met de situatie dat een fraudeur er in slaagt een bankrekening te openen op andermans naam. In het licht van de column van Jaap-Henk is het daarom opvallend dat juist de federatieve opzet van Idensys een antwoord kan bieden op deze kwestie. Dit antwoord bestaat uit een centrale dienst voor burgers waar zij (onder pseudoniem) kunnen zien bij welke authenticatiediensten zij middelen hebben geregistreerd. De federatieve opzet maakt het aanloggen bij deze dienst eenvoudig. Een onjuist afgegeven middel wordt dan direct zichtbaar. Verder zou het mogelijk kunnen zijn dat een gebruiker bij de inzagedienst expliciet aangeeft geen gebruik te willen maken van bepaalde middelen of over de verstrekking daarvan wenst te worden genotificeerd. Feitelijk is deze dienst daarmee een sterke inrichting van het recht op inzage zoals verankerd in artikel 35 van de Wet bescherming persoonsgegevens. De opzet van deze inzagedienst, waar ik aandacht voor vraag binnen het Idensys doorgroei programma, heeft volgens mij geen evenknie in het niet-federatieve voorstel van Jaap-Henk. Tenminste, als we niet uitgaan van een overheid die maar één type authenticatiemiddel toelaat. In die zin is het eigenlijk wel ironisch dat het belangrijkste zorgpunt dat Jaap-Henk oppert in zijn column fundamenteler in zijn eigen voorstel is dan binnen een federatie.

Uit bovenstaand iDEAL voorbeeld wordt ook het voordeel van federatieve authenticatie duidelijk: de dienstverlener hoeft alleen de gestandaardiseerde berichten te kunnen ontvangen/lezen en hoeft zich niet te verdiepen in de specifieke details om met het middel te kunnen praten. Voor de dienstverlener betekent federatieve authenticatie daarom dat hij ruime flexibiliteit heeft in het toestaan van middelen. Waar de dienstverlener in het voorstel van Jaap-Henk voor elk nieuw middel zich zou moeten verdiepen in de technische details om met het middel te communiceren, hoeft hij bij federatieve authenticatie alleen maar identiteit berichten van de betreffende authenticatiedienst toe te staan. Dit voordeel komt ten goede aan de gebruikersvriendelijkheid en laagdrempeligheid van federatieve authenticatie: de gebruiker heeft veel flexibiliteit om een middel te gebruiken dat het beste past bij zijn omstandigheden. Hij kan een smartcard gebruiken bij zijn PC, en een smartphone/SMS bij zijn tablet et cetera. In dit verband merken wij nog op dat juist de laagdrempeligheid de reden was van het grote succes achter DigiD. Met de federatieve keuze van Idensys wordt precies hetzelfde nagestreefd.

De column beschrijft wel een ander, en terecht, zorgpunt rond de privacy bescherming binnen een federatief stelsel. Dit punt is dat in een basale federatieve implementatie de authenticatiedienst zowel weet wie de klant is als

wel waar deze aanlogt. Dat is vergelijkbaar met de situatie dat uw bank weet waar u aankopen heeft gedaan met uw betaalpas of via iDEAL. Dit zorgpunt is onderkend in zowel de Idensys risico analyse [5.] als in de Privacy Impact Assessment [6.]. Het wordt ook genoemd in de berichten standaard (SAMLv2, zie [7.]) die de basis vormt voor Idensys.

Het is zeker zo dat deze kwestie in een niet-federatieve opzet eenvoudiger is op te lossen dan in een federatieve opzet. Dit juist omdat de authenticatiedienst een minder actieve rol speelt bij de niet-federatieve opzet. Dit zorgpunt van federatieve authenticatie heeft grote aandacht in de doorgroei van Idensys. Daarbij is ook al reeds in 2014 een technische oplossing geïdentificeerd die dit zorgpunt kan gaan oplossen in de vorm van polymorfe pseudonimisering [9.]. In de sterkste toepassing hiervan kan de authenticatiedienst wel actief zijn tussen gebruiker en dienstverlener zonder de identiteit van de gebruiker te kunnen achterhalen of zelfs maar te kunnen vaststellen of tweemaal dezelfde klant wordt geholpen. Toepassing van deze opzet op de Nederlandse identiteitsdocumenten behoort daarbij tot de mogelijkheden. Daarbij kan ook gebruik worden gemaakt van "*proven technology*" zoals die al op het Nederlandse paspoort wordt gebruikt. In die zin kan binnen Idensys het beste gehaald worden uit twee werelden: de gebruiksvriendelijkheid en laagdrempeligheid van federatieve authenticatie en de privacy bescherming van niet-federatieve authenticatie. Polymorfe pseudonimisering kan ook verdere privacy bescherming bieden bij bestaande middelen omdat het een sterke scheiding mogelijk maakt bij een authenticatiedienst tussen klant- en middelregistraties. Het zijn juist deze toepassingen waar ik aandacht voor vraag binnen het Idensys doorgroei programma.

Het is geen geheim dat Jaap-Henk een warm voorstander is van de IRMA kaart zoals die ontwikkeld is vanuit de Radboud universiteit. En het is ontegenzeggelijk zo dat de IRMA kaart unieke en bijzonder sterke privacy eigenschappen heeft. Maar mijn inziens hindert de niet-federatieve opzet van de kaart diens massale uitrol, zelfs als deze in als een smartphone APP zou worden geïmplementeerd waarmee nu wordt geëxperimenteerd. Het goede nieuws is echter dat ook de IRMA kaart binnen Idensys (dus federatief) kan worden gebruikt zonder verlies van diens privacy eigenschappen. Dit heb ik gepresenteerd op de IRMA bijeenkomst van 22 mei 2015. Zie [8.]. Met deze opzet zou ook de IRMA kaart laagdrempelig kunnen worden ingezet. Kortom, de tegenstelling tussen federatieve en niet-federatieve authenticatie is minder groot dan men denkt. In plaats van een stammenstrijd aan te gaan zou mijn voorstel zijn dat beide kampen samen verder optrekken en waarbij de IRMA opzet federatief wordt aangesloten op Idensys.

Tot slot wil ik nog opmerken dat ik de signalen in de column van Jaap-Henk op prijs stel, juist omdat zij mij helpen mijn bijdrage te leveren bij een privacy-vriendelijke doorontwikkeling van Idensys.

Referenties	
#	Document
[1.]	http://fd.nl/morgen/1138342/wilt-u-af-van-de-authenticatie-pooier
[2.]	https://afsprakenstelsel.etoegang.nl/display/as/Eisen+aan+middelen
[3.]	VERORDENING (EU) Nr. 910/2014 VAN HET EUROPEES PARLEMENT EN DE RAAD van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG. Zie https://ec.europa.eu/digital-agenda/en/trust-services-and-eid.
[4.]	UITVOERINGSVERORDENING (EU) 2015/1502 VAN DE COMMISSIE van 8 september 2015 tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen. Zie https://ec.europa.eu/digital-agenda/en/trust-services-and-eid.
[5.]	https://afsprakenstelsel.etoegang.nl/display/as/Stelselrisicoanalyse
[6.]	https://www.idensys.nl/fileadmin/bestanden/idensys/documenten/basisdocumentatie/pia/Privacy_impactanalyse_eID_Stelsel.pdf
[7.]	http://docs.oasis-open.org/security/saml/v2.0/saml-sec-consider-2.0-os.pdf
[8.]	https://www.cs.ru.nl/E.Verheul/presentations/IRMA_federated.pdf
[9.]	https://www.cs.ru.nl/E.Verheul/presentations/The_Dutch_eID.pdf